Cisco Configuration Professional: Firewall Zona-baseado que obstrui o par para espreitar exemplo de configuração do tráfego

Índice

Introdução

Este documento fornece uma aproximação passo a passo para configurar um roteador do Cisco IOS como um Firewall zona-baseado para obstruir o tráfego (P2P) peer-to-peer usando o assistente avançado da configuração de firewall no Cisco Configuration Professional (Cisco CP).

O Firewall Zona-baseado da política (igualmente conhecido como o Firewall da Zona-política, ou o ZFW) muda a configuração de firewall do modelo relação-baseado mais velho a um modelo zona-baseado mais flexível, mais de fácil compreensão. As relações são atribuídas às zonas, e a política da inspeção é aplicada para traficar mover-se entre as zonas. as políticas da Inter-zona oferecem a flexibilidade e a granularidade consideráveis. Consequentemente, as políticas diferentes da inspeção podem ser aplicadas aos grupos do host múltiplo conectados à relação do mesmo roteador. As zonas estabelecem as beiras da Segurança de sua rede. Uma zona define um limite onde o tráfego seja sujeitado às limitações da política como ele se cruze a uma outra região de sua rede. A política padrão de ZFW entre zonas é nega tudo. Se nenhuma política é configurada explicitamente, todo o tráfego que se move entre zonas está obstruído.

Os aplicativos P2P são alguns dos aplicativos os mais amplamente utilizados no Internet. As redes P2P podem atuar como uma conduíte para ameaças maliciosas tais como worms, oferecendo um trajeto fácil em torno dos Firewall e causando interesses sobre a privacidade e a Segurança. Apoio introduzido Cisco IOS Software Release 12.4(9)T ZFW para aplicativos P2P. A inspeção P2P oferece políticas da camada 4 e da camada 7 para o tráfego de aplicativo. Isto significa que ZFW pode fornecer a inspeção stateful básica ao permit or deny o tráfego, assim

como o controle granulado da camada 7 em atividades específicas nos vários protocolos, de modo que determinadas atividades do aplicativo sejam permitidas quando outro forem negadas.

Cisco CP oferece uma aproximação fácil de seguir, passo a passo configurar o IOS Router como um Firewall zona-baseado usando o assistente avançado da configuração de firewall.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O IOS Router deve ter a versão de software como 12.4(9)T ou mais tarde.
- Para os modelos do IOS Router que apoiam Cisco CP, refira os Release Note de Cisco CP.

Configuração de roteador para dirigir Cisco CP

Nota: Execute estas etapas de configuração a fim dirigir Cisco CP em um roteador Cisco:

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
Router(config)# username <username> privilege 15 password 0 <password>
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- IOS Router de Cisco 1841 que executa a IOS Software release 12.4(15)T
- 2.1 da liberação do Cisco Configuration Professional (Cisco CP)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Para o exemplo deste documento, o roteador é configurado como um Firewall zona-baseado para obstruir o tráfego P2P. O roteador ZFW tem duas relações, uma relação do inside(trusted) na Em-zona e uma relação (não confiável) exterior na Para fora-zona. O roteador ZFW obstrui pedidos

P2P tais como o edonkey, o fasttrack, o gnutella e o kazaa2 com ação de registro para o tráfego que está passando da Em-zona à Para fora-zona.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configuração através do Cisco Configuration Professional

Esta seção contém o procedimento passo a passo em como usar o assistente para configurar o IOS Router como um Firewall zona-baseado.

Conclua estes passos:

1. Vá **configurar o > segurança > o Firewall e o ACL**. Então, escolha o botão de rádio **avançado do Firewall**. Clique o **lançamento a tarefa selecionada**.
2. Esta tela seguinte mostra uma breve introdução sobre o assistente do Firewall. Clique **ao lado do** começo que configura o Firewall.
3. Selecione as relações do roteador para ser parte de zonas e clique-as **em seguida**.
4. A política padrão com segurança elevada junto com o conjunto de comandos é mostrada na próxima janela. O clique **perto de** continua.
5. Incorpore os detalhes do servidor DNS e clique-os **em seguida**.
6. Cisco CP fornece um sumário de configuração tal como esse mostrado aqui. **Revestimento do** clique para terminar a configuração.O sumário da configuração detalhada é fornecido nesta tabela. Esta é a configuração padrão conforme a política de segurança elevada de Cisco CP.
7. Verifique a **salvaguarda a configuração running à** caixa de verificação da **configuração de inicialização do roteador**. O clique **entrega** para enviar esta configuração ao roteador.A configuração completa é entregada ao roteador. Isto toma algum tempo para processar.
8. **APROVAÇÃO do** clique a continuar.
9. **APROVAÇÃO do** clique outra vez.A configuração é agora de fato e é mostrada como as regras sob a aba da política de firewall.
10. As zonas junto com os pares que da zona são associadas podem ser vistas se você vai **configurar o > segurança > a segurança avançada > as zonas**. Você pode igualmente adicionar zonas novas clicando **adiciona**, ou altera as zonas existentes clicando **edita**.
11. Vá **configurar o > segurança > os pares da segurança avançada > da zona** para ver os detalhes dos pares da zona.A ajuda imediata em como alterar/adicionam/zonas da supressão/pares da zona e a outra informação relacionada está prontamente - disponível com os página da web incorporados em Cisco CP.
12. A fim alterar com certeza os aplicativos característicos da aplicação P2P das capacidades

da inspeção, vá ao **> segurança da configuração > ao Firewall e ao ACL**. Então, o clique **edita a política de firewall** e escolhe a regra respectiva no mapa de política. O clique **edita**.Isto mostra aos aplicativos atuais P2P que à revelia configuração obstruída.
13. Você pode usar adicionar e os botões Remove Button a adicionar/removem os aplicativos específicos. Este tiro de tela mostra como adicionar o aplicativo do winmx obstruir isso.
14. Em vez de escolher a ação de queda, você pode igualmente escolher a ação da inspeção aplicar opções diferentes para a inspeção de pacote de informação profunda.A inspeção P2P oferece políticas da camada 4 e da camada 7 para o tráfego de aplicativo. Isto significa que ZFW pode fornecer a inspeção stateful básica ao permit or deny o tráfego, assim como o controle granulado da camada 7 em atividades específicas nos vários protocolos, de modo que determinadas atividades do aplicativo sejam permitidas quando outro forem negadas. Nesta inspeção de aplicativo, você pode aplicar tipos diferentes de inspeçãos específicas do nível do encabeçamento para aplicativos P2P. Um exemplo para o gnutella é mostrado em seguida.
15. Verifique a opção **P2P** e o clique **cria** a fim criar um mapa de política novo para este.
16. Crie um mapa de política novo para a inspeção de pacote de informação profunda para o protocolo do gnutella. O clique **adiciona** e escolhe então o **mapa novo da classe**.
17. Dê um novo nome para o mapa de classe e o clique **adiciona** para especificar critérios de verificação de repetição de dados.
18. Use transferência de arquivo porque o critério do fósforo e a corda usados são .exe. Isto indica que todas as conexões de transferência de arquivo do gnutella que contêm a série de compatibilidade do .exe para a política de tráfego. Clique em **OK**.
19. **APROVAÇÃO do** clique outra vez para terminar a configuração de mapa de classe.
20. Escolha a **restauração** ou **permita a** opção, que depende da política de segurança de sua empresa. Clique a **APROVAÇÃO** para confirmar a ação com o mapa de política.Nesta mesma maneira você pode adicionar outros política-mapas para executar características profundas da inspeção para outros protocolos P2P especificando expressões regulares diferentes como o critério do fósforo.**Nota:** Os aplicativos P2P são particularmente difíceis de detectar, em consequência do comportamento da “porta-lupulagem” e dos outros truques para evitar a detecção, assim como dos problemas introduzidos por mudanças e por atualizações frequentes aos aplicativos P2P que alteram os comportamentos dos protocolos. ZFW combina a inspeção stateful nativa do Firewall com capacidades do tráfego-reconhecimento s do Network-Based Application Recognition (NBAR) 'de entregar o controle de aplicativo P2P.**Nota:** A inspeção de aplicativo P2P oferece capacidades características da aplicação para um subconjunto dos aplicativos apoiados pela inspeção da camada 4:edonkeyfasttrackgnutellakazaa2**Nota:** Atualmente, ZFW não tem uma opção para inspecionar o tráfego de aplicativo “bittorrent”. Os clientes de BitTorrent comunicam-se geralmente com os perseguidores (servidores de diretório do par) através do HTTP que é executado em alguma porta não padronizada. Este é tipicamente TCP 6969, mas você pôde precisar de verificar a porta torrente-específica do perseguidor. Se você deseja permitir BitTorrent, o melhor método para acomodar a porta adicional é configurar o HTTP como um dos protocolos do fósforo e adicionar TCP 6969 ao HTTP usando este comando ip port-map: **porta tcp 6969 HTTP do mapa de porta IP**. Você precisará de definir o HTTP e bitTorrent como os critérios de verificação de repetição de dados aplicados no mapa de classe.
21. Clique a **APROVAÇÃO** para terminar a configuração avançada da inspeção.O conjunto de comandos correspondente é entregado ao roteador.
22. Clique a **APROVAÇÃO** para terminar o copi do conjunto de comandos ao roteador.

23. Você pode observar as regras novas ocorrer da aba da política de firewall da edição abaixo **para configurar o > segurança > o Firewall e o ACL**.

Comando line configuration do roteador ZFW

A configuração na seção anterior de Cisco CP conduz a esta configuração no roteador ZFW:

Roteador ZBF

```
ZBF-Router#show run
Building configuration...

Current configuration : 9782 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ZBF-Router
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
ip cef
!
!
!
!
ip name-server 10.77.230.45
!
multilink bundle-name authenticated
parameter-map type protocol-info msn-servers
 server name messenger.hotmail.com
 server name gateway.messenger.hotmail.com
 server name webmessenger.msn.com

parameter-map type protocol-info aol-servers
 server name login.oscar.aol.com
 server name toc.oscar.aol.com
 server name oam-d09a.blue.aol.com

parameter-map type protocol-info yahoo-servers
 server name scs.msg.yahoo.com
 server name scsa.msg.yahoo.com
 server name scsb.msg.yahoo.com
 server name scsc.msg.yahoo.com
 server name scsd.msg.yahoo.com
 server name cs16.msg.dcn.yahoo.com
 server name cs19.msg.dcn.yahoo.com
 server name cs42.msg.dcn.yahoo.com
 server name cs53.msg.dcn.yahoo.com
 server name cs54.msg.dcn.yahoo.com
 server name ads1.vip.scd.yahoo.com
 server name radio1.launch.vip.dal.yahoo.com
 server name in1.msg.vip.re2.yahoo.com
 server name data1.my.vip.sc5.yahoo.com
 server name address1.pim.vip.mud.yahoo.com
 server name edit.messenger.yahoo.com
```

```
 server name messenger.yahoo.com
 server name http.pager.yahoo.com
 server name privacy.yahoo.com
 server name csa.yahoo.com
 server name csb.yahoo.com
 server name csc.yahoo.com

parameter-map type regex ccp-regex-nonascii
 pattern [^\x00-\x80]

!
!
!
crypto pki trustpoint TP-self-signed-1742995674
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1742995674
 revocation-check none
 rsakeypair TP-self-signed-1742995674
!
!
crypto pki certificate chain TP-self-signed-1742995674
 certificate self-signed 02
  30820242 308201AB A0030201 02020102 300D0609 2A864886
F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967
6E65642D 43657274
  69666963 6174652D 31373432 39393536 3734301E 170D3130
31313236 31303332
  32315A17 0D323030 31303130 30303030 305A3031 312F302D
06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361
74652D31 37343239
  39353637 3430819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281
  8100A84A 980D15F0 6A6B5F1B 5A3359DE 5D552EFE FAA8079B
DA927DA2 4AF210F0
  408131CE BB5B0189 FD82E22D 6A6284E3 5F4DB2A7 7517772B
1BC5624E A1A6382E
  6A07EE71 E93A98C9 B8494A55 0CDD6B4C 442065AA DBC9D9CC
14D10B65 2FEFECC8
  AA9B3064 59105FBF B9B30219 2FD53ECA 06720CA1 A6D30DA5
564FCED4 C53FC7FD
  835B0203 010001A3 6A306830 0F060355 1D130101 FF040530
030101FF 30150603
  551D1104 0E300C82 0A5A4246 2D526F75 74657230 1F060355
1D230418 30168014
  0BDBE585 15377DCA 5F00A1A2 6644EC22 366DE590 301D0603
551D0E04 1604140B
  DBE58515 377DCA5F 00A1A266 44EC2236 6DE59030 0D06092A
864886F7 0D010104
  05000381 810037F4 8EEC7AF5 85429563 F78F2F41 A060EEE8
F23D8F3B E0913811
  A143FC44 8CCE71C3 A5E9D979 C2A8CD38 C272A375 4FCD459B
E02A9427 56E2F1A0
  DA190B50 FA091669 CD8C066E CD1A095B 4E015326 77B3E567
DFD55A71 53220F86
  F006D31E 02CB739E 19D633D6 61E49866 C31AD865 DC7F4380
FFEDDBAB 89E3B3E9
  6139E472 DC62
        quit
!
!
username cisco privilege 15 password 0 cisco123
archive
```

```
 log config
  hidekeys
!
!
class-map type inspect match-all sdm-cls-im
 match protocol ymsgr
class-map type inspect imap match-any ccp-app-imap
 match  invalid-command
class-map type inspect match-any ccp-cls-protocol-p2p
 match protocol  signature
 match protocol gnutella signature
 match protocol kazaa2 signature
 match protocol fasttrack signature
 match protocol bitTorrent signature
class-map type inspect smtp match-any ccp-app-smtp
 match  data-length gt 5000000
class-map type inspect http match-any ccp-app-nonascii
 match  req-resp header regex ccp-regex-nonascii
class-map type inspect match-any CCP-Voice-permit
 match protocol h323
 match protocol skinny
 match protocol sip
class-map type inspect gnutella match-any ccp-class-
gnutella
 match  file-transfer .exe
class-map type inspect match-any ccp-cls-insp-traffic
 match protocol dns
 match protocol https
 match protocol icmp
 match protocol imap
 match protocol pop3
 match protocol tcp
 match protocol udp
class-map type inspect match-all ccp-insp-traffic
 match class-map ccp-cls-insp-traffic
class-map type inspect match-any ccp-cls-icmp-access
 match protocol icmp
 match protocol tcp
 match protocol udp
!!--- Output suppressed ! class-map type inspect match-
all sdm-cls-p2p match protocol gnutella class-map type
inspect match-all ccp-protocol-pop3 match protocol pop3
class-map type inspect kazaa2 match-any ccp-cls-p2p
match file-transfer class-map type inspect pop3 match-
any ccp-app-pop3 match invalid-command class-map type
inspect match-all ccp-protocol-p2p match class-map ccp-
cls-protocol-p2p class-map type inspect match-all ccp-
protocol-im match class-map ccp-cls-protocol-im class-
map type inspect match-all ccp-invalid-src match access-
group 100 class-map type inspect match-all ccp-icmp-
access match class-map ccp-cls-icmp-access class-map
type inspect http match-any ccp-app-httpmethods match
request method bcopy match request method bdelete match
request method bmove match request method bpropfind
match request method bproppatch match request method
connect match request method copy match request method
delete match request method edit match request method
getattribute match request method getattributenames
match request method getproperties match request method
index match request method lock match request method
mkcol match request method mkdir match request method
move match request method notify match request method
options match request method poll match request method
post match request method propfind match request method
```

```
proppatch match request method put match request method
revadd match request method revlabel match request
method revlog match request method revnum match request
method save match request method search match request
method setattribute match request method startrev match
request method stoprev match request method subscribe
match request method trace match request method unedit
match request method unlock match request method
unsubscribe class-map type inspect http match-any ccp-
http-blockparam match request port-misuse im match
request port-misuse p2p match request port-misuse
tunneling match req-resp protocol-violation class-map
type inspect match-all ccp-protocol-imap match protocol
imap class-map type inspect match-all ccp-protocol-smtp
match protocol smtp class-map type inspect match-all
ccp-protocol-http match protocol http ! ! policy-map
type inspect ccp-permit-icmpreply class type inspect
ccp-icmp-access inspect class class-default pass ! !--- 
Output suppressed ! policy-map type inspect http ccp-
action-app-http class type inspect http ccp-http-
blockparam log reset class type inspect http ccp-app-
httpmethods log reset class type inspect http ccp-app-
nonascii log reset class class-default policy-map type
inspect smtp ccp-action-smtp class type inspect smtp
ccp-app-smtp reset class class-default policy-map type
inspect imap ccp-action-imap class type inspect imap
ccp-app-imap log reset class class-default policy-map
type inspect pop3 ccp-action-pop3 class type inspect
pop3 ccp-app-pop3 log reset class class-default policy-
map type inspect ccp-inspect class type inspect ccp-
invalid-src drop log class type inspect ccp-protocol-
http inspect service-policy http ccp-action-app-http
class type inspect ccp-protocol-smtp inspect service-
policy smtp ccp-action-smtp class type inspect ccp-
protocol-imap inspect service-policy imap ccp-action-
imap class type inspect ccp-protocol-pop3 inspect
service-policy pop3 ccp-action-pop3 class type inspect
sdm-cls-p2p inspect ! !--- Output suppressed ! class
type inspect ccp-protocol-im drop log class type inspect
ccp-insp-traffic inspect class type inspect CCP-Voice-
permit inspect class class-default pass policy-map type
inspect ccp-permit class class-default policy-map type
inspect p2p ccp-pmap-gnutella class type inspect
gnutella ccp-class-gnutella ! zone security out-zone
zone security in-zone zone-pair security ccp-zp-self-out
source self destination out-zone service-policy type
inspect ccp-permit-icmpreply zone-pair security ccp-zp-
in-out source in-zone destination out-zone service-
policy type inspect ccp-inspect zone-pair security ccp-
zp-out-self source out-zone destination self service-
policy type inspect ccp-permit ! ! ! interface
FastEthernet0/0 description $FW_OUTSIDE$ ip address
209.165.201.2 255.255.255.224 zone-member security out-
zone duplex auto speed auto ! interface FastEthernet0/1
description $FW_INSIDE$ ip address 10.77.241.114
255.255.255.192 zone-member security in-zone duplex auto
speed auto ! ! !--- Output suppressed ! ! ip http server
ip http authentication local ip http secure-server ! !
!--- Output suppressed ! ! ! control-plane ! ! line con
0 line aux 0 line vty 0 4 privilege level 15 login local
transport input ssh ! scheduler allocate 20000 1000 !
webvpn cef end ZBF-Router#
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **O tipo do mapa de política de** ZBF-Router#show **inspeciona sessões dos zona-pares** — Indica o tempo de execução inspecionam o tipo estatísticas do mapa de política para todos os pares existentes da zona.

Informações Relacionadas

- Projeto do Firewall da política e guia Zona-baseados do aplicativo
- Exemplo virtual clássico e Zona-baseado do Cisco IOS Firewall do Firewall da configuração do aplicativo
- Home Page do Cisco Configuration Professional
- Guia do Usuário do Cisco Configuration Professional
- Suporte Técnico e Documentação - Cisco Systems